UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,744	12/30/2003	Yang Seo Choi	2013P146	9025

8791 7590 12/21/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
LE, CANH	
ART UNIT	PAPER NUMBER
2112	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/21/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/749,744	CHOI ET AL.	
	Examiner	Art Unit	
	Canh Le	2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/30/2003*; 02/23/2004; 10/19/2005
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

The disclosure is objected to because of the following informalities: The Examiner does not understand a phrase "port number of the **response packet**" in a paragraph [0052]. Please, review the translation for appropriateness. Appropriate correction is required.

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract has more than 150 words. Appropriate correction is required.

Claim Objections

Claim 1 is objected to because of the following informalities: A system appears twice in this claim. "**a system** attack sensing signal ... to **a system** and a first response packet". Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 14 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. A readable medium includes carrier waves (see paragraph [0064]) and "carrier waves" are, per se, non-statutory.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Wang et al., "Tracing Based Active Intrusion Response", obtained from

http://argos.csc.ncsu.edu/papers/2001-09-sleepytracing-jiw.pdf, September-2001, pages 1-11, herein after TBAIR.

Claim 1

TBAIR discloses a traceback connection apparatus comprising:

a packet blocking unit, which if a system attack sensing signal is received, blocks an attack packet transmitted to a system and a first response packet output from the system in response to the attack packet (Pages 7-8, section 5; Remote blocking and containment);

a response packet generation unit, which generates a second response packet into which a watermark is inserted, in response to the attack packet, and transmits the second response packet to a system corresponding to the source address of the attack packet (Pages 5-7, section 4-4.2; Pages 8-9, section 6; where an watermark-enabled application injects a watermark into a backward traffic of an intrusion connection); and

a path traceback unit, which receives a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, traces back the transmission path of the second response packet and identifies the location of the attacker system (Pages 5-7, section 4-4.2; Pages 7-8, section 5).

Claim 2

TBAIR discloses the apparatus of claim 1, further comprising:

an attack detection unit, which if a system attack by an external attacker is sensed, outputs an attack sensing signal containing the IP addresses of the source and destination of the attack path and the port number (Pages 5-7, section 4-4.2; Pages 7-8, section 5).

Claim 3

TBAIR discloses the apparatus of claim 2, wherein the attack detection unit senses a system attack by the external attacker by investigating log files of the system, log files of a network, and whether or not a predetermined system file has been changed, and based on the log file of the system, identifies the IP address of the source and port number of the attack packet (Pages 5-6, section 4-4.2; Pages 7-8, section 5; Remote decoy and trap).

Claim 4

TBAIR discloses the apparatus of claim 2, wherein the packet blocking unit comprises:

a signal reception unit, which receives the attack sensing signal (Pages 5-7, section 4-4.2; Pages 7-8, section 5; Remote monitoring and surveillance);

a packet identifying unit, which identifies the attack packet and the first response packet based on the IP addresses and the port number (Pages 5-7, section 4-4.2; Pages 7-8, section 5); and

a blocking unit, which blocks the attack packet and the first response packet (Pages 7-8, section 5; Remote blocking and containment).

Claim 5

TBAIR discloses the apparatus of claim 1, further comprising:

a watermark detection unit, which if a packet containing a watermark from an external network is received, transmits a detection packet containing the path information of the received packet to a system of the external network which inserted the watermark (Pages 5-7, section 4-4.2; Page 7, section 5).

Claim 6

TBAIR discloses the apparatus of claim 5, wherein the watermark detection unit comprises:

a detection unit, which detects a watermark contained in a packet received from the outside (Pages 5-7, section 4-4.2; Page 7, section 5; Remote monitoring and surveillance);

a detection packet generation unit, which if a watermark is detected, generates a detection packet containing the IP addresses of the source and destination and port number of the received packet (Pages 5-6, section 4); and

a packet transmission unit, which transmits the generated detection packet to a system that first inserted the watermark to the packet (Pages 5-6, section 4; Pages 7-8, section 5; Remote monitoring and surveillance).

Claim 7

TBAIR discloses the apparatus of claim 1, wherein the path traceback unit traces back the location of an attacker system based on the IP addresses of the source and destination and port number contained in the one or more received detection packets (Pages 5-7, section 4-4.2).

Claim 8

TBAIR discloses a traceback connection method comprising:

blocking an attack packet transmitted to the system and a first response packet output from a system in response to the attack packet, if a system invasion sensing signal is received (Pages 7-8, section 5; Remote blocking and containment);

generating a second response packet into which a watermark is inserted, in response to the attack packet, and transmitting the second response packet to a system corresponding to the source address of the attack packet (Pages 5-7, section 4-4.2; Pages 8-9, section 6; where an watermark-enabled application injects a watermark into a backward traffic of an intrusion connection); and

receiving a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, tracing back the transmission path of the second response packet and identifying the location of the

attacker system (Pages 5-7, section 4-4.2; Pages 7-8, section 5).

Claim 9

TBAIR discloses the method of claim 8, further comprising:

outputting an attack sensing signal containing the IP addresses of the source and destination of the attack path and the port number before the blocking, if a system attack by an external attacker is sensed (Pages 5-7, section 4-4.2; Pages 7-8, section 5).

Claim 10

TBAIR discloses the method of claim 9, wherein the blocking comprises:

receiving the attack sensing signal (Pages 5-7, section 4-4.2; Pages 7-8, section 5; Remote monitoring and surveillance);

identifying the attack packet and the first response packet based on the IP addresses and the port number (Pages 5-7, section 4-4.2; Pages 7-8, section 5); and

blocking the attack packet and the first response packet (Pages 7-8, section 5; Remote blocking and containment).

Claim 11

TBAIR discloses the method of claim 8, further comprising:

transmitting a predetermined detection packet to a system of the external network which inserted the watermark, if a packet containing a watermark from an

external network is received (Pages 5-7, section 4-4.2; Page 7, section 5).

Claim 12

TBAIR discloses the method of claim 11, wherein transmitting a detection packet comprises:

detecting a watermark contained in a receive packet (Pages 5-7, section 4-4.2; Page 7, section 5; Remote monitoring and surveillance);

If the watermark is detected, generating a detection packet containing the IP addresses of the source and destination and port number of the received packet (Pages 5-6, section 4); and

transmitting the generated detection packet to a system that first inserted the watermark to the packet (Pages 5-6, section 4; Pages 7-8, section 5; Remote monitoring and surveillance).

Claim 13

TBAIR discloses the method of claim 8, wherein the tracking back the transmission path comprises:

tracking back the location of an attacker system based on the IP addresses of the source and destination and port number contained in the one or more received detection packets (Pages 5-7, section 4-4.2).

Claim 14

TBAIR discloses a computer readable medium having embodied thereon a computer program for executing a traceback connection method comprising (Pages 5, section 4-4.2; routers):

blocking an attack packet transmitted to the system and a first response packet output from the system as a response to the attack packet, if a system invasion sensing signal is received;

generating a second response packet into which a watermark is inserted, in response to the attack packet, and transmitting the second response packet to a system corresponding to the source address of the attack packet; and

receiving a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, tracing back the transmission path of the second response packet and identifying the location of the attacker system.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Choi et al. (Publication No.: US 20040049695 A1).

Claim 1

Choi discloses a traceback connection apparatus comprising:

a packet blocking unit, which if a system attack sensing signal is received, blocks an attack packet transmitted to a system and a first response packet output from the system in response to the attack packet (Abstract; Paragraph [0009], lines 6-9; Paragraph [0010], lines 5-16; Figure 4, box 420);

a response packet generation unit, which generates a second response packet into which a watermark is inserted, in response to the attack packet, and transmits the second response packet to a system corresponding to the source address of the attack packet (Abstract; Paragraph [0008], lines 4-5; Paragraph [0009], lines 24-25; where a watermark inserts into a response packet); and

a path traceback unit, which receives a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, traces back the transmission path of the second response packet and identifies the location of the attacker system (Abstract; Paragraph [0009], line 8; Paragraph [0010], lines 5-17; Figure 2, box 230; Figure 4, box 430).

Claim 2

Choi discloses the apparatus of claim 1, further comprising:

an attack detection unit, which if a system attack by an external attacker is sensed, outputs an attack sensing signal containing the IP addresses of the source and destination of the attack path and the port number (Abstract; Paragraph [0009], lines 10-12; Paragraph [0010], lines 5-13; Figure 2, box 210; Figure 3, box 310).

Claim 3

Choi discloses the apparatus of claim 2, wherein the attack detection unit senses a system attack by the external attacker by investigating log files of the system, log files of a network, and whether or not a predetermined system file has been changed, and based on the log file of the system, identifies the IP address of the source and port number of the attack packet (Paragraph [0009], lines 8-12; where collecting a response packet from the attacked system is equivalent to a log file of system).

Claim 4

Choi discloses the apparatus of claim 2, wherein the packet blocking unit comprises:

a signal reception unit, which receives the attack sensing signal (Abstract; Paragraph [0009], lines 10-11; Paragraph [0010], lines 5-13; Figure 2, box 210; Figure 3, box 310);

a packet identifying unit, which identifies the attack packet and the first response

packet based on the IP addresses and the port number (Abstract; Paragraph [0009], lines 10-11; Paragraph [0010], lines 5-13; Figure 2, box 210; Figure 3, box 310); and

a blocking unit, which blocks the attack packet and the first response packet (Abstract; Paragraph [0009], lines 10-11; Paragraph [0010], lines 5-13; Figure 2, box 210; Figure 3, box 310).

Claim 5

Choi discloses the apparatus of claim 1, further comprising:

a watermark detection unit, which if a packet containing a watermark from an external network is received, transmits a detection packet containing the path information of the received packet to a system of the external network which inserted the watermark (Abstract; Paragraph [0009], line 11; Paragraph [0010], lines 22-23; Figure 2, box 240; Figure 4, box 440).

Claim 6

Choi discloses the apparatus of claim 5, wherein the watermark detection unit comprises:

a detection unit, which detects a watermark contained in a packet received from the outside (Paragraph [0025]);

a detection packet generation unit, which if a watermark is detected, generates a detection packet containing the IP addresses of the source and destination and port number of the received packet (Paragraph [0025]); and

a packet transmission unit, which transmits the generated detection packet to a system that first inserted the watermark to the packet (Paragraph [0025]). The Examiner gives abroad interpretation of the watermark detection unit. It includes the detection unit, a detection packet generation unit, and a packet transmission unit.

Claim 7

Choi discloses the apparatus of claim 1, wherein the path traceback unit traces back the location of an attacker system based on the IP addresses of the source and destination and port number contained in the one or more received detection packets (Figure 2, box 220, box 230; Figure 4, box 420, box 430; Paragraph [0009], lines 9-18; where an ID address is equivalent to an IP address and a packet block unit is connect with a path tracing unit).

Claim 8

Choi discloses a traceback connection method comprising:

blocking an attack packet transmitted to the system and a first response packet output from a system in response to the attack packet, if a system invasion sensing signal is received (Abstract; Paragraph [0009], lines 6-9; Paragraph [0010], lines 5-16);

generating a second response packet into which a watermark is inserted, in response to the attack packet, and transmitting the second response packet to a system corresponding to the source address of the attack packet (Abstract;

Paragraph [0008], lines 4-5; Paragraph [0009], lines 24-25; where a watermark inserts into a response packet); and

receiving a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, tracing back the transmission path of the second response packet and identifying the location of the attacker system (Abstract; Paragraph [0009], line 8-25; Paragraph [0010], lines 5-17).

Claim 9

Choi discloses the method of claim 8, further comprising:

outputting an attack sensing signal containing the IP addresses of the source and destination of the attack path and the port number before the blocking, if a system attack by an external attacker is sensed (Abstract; Paragraph [0009], lines 10-19; Paragraph [0010], lines 5-14; where an ID address is equivalent to an IP address).

Claim 10

Choi discloses the method of claim 9, wherein the blocking comprises:

receiving the attack sensing signal (Paragraph [0009], lines 6-7; Paragraph [0010], lines 7-9);

identifying the attack packet and the first response packet based on the IP addresses and the port number (Paragraph [0009], lines 7-10; Paragraph [0010], lines 9-13); and

blocking the attack packet and the first response packet (Paragraph [0009], lines 6-7; Paragraph [0010], lines 14-16).

Claim 11

Choi discloses the method of claim 8, further comprising:

transmitting a predetermined detection packet to a system of the external network which inserted the watermark, if a packet containing a watermark from an external network is received (Abstract; Paragraph [0009], line 19-25; Paragraph [0010], lines 20-24;).

Claim 12

Choi discloses the method of claim 11, wherein transmitting a detection packet comprises:

detecting a watermark contained in a receive packet (Paragraph [0025);

If the watermark is detected, generating a detection packet containing the IP addresses of the source and destination and port number of the received packet (Paragraph [0025]); and

transmitting the generated detection packet to a system that first inserted the watermark to the packet (Paragraph [0025]).

Claim 13

Choi discloses the method of claim 8, wherein the tracking back the transmission path comprises:

tracking back the location of an attacker system based on the IP addresses of the source and destination and port number contained in the one or more received detection packets (Figure 2, box 220, box 230; Figure 4, box 420, box 430; Paragraph [0009], lines 9-13; where an ID address is equivalent to an IP address and a packet block unit is connect with a path tracing unit).

Claim 14

Choi discloses a computer readable medium having embodied thereon a computer program for executing a traceback connection method comprising (Paragraph [0009], lines 11-13; Paragraph [0010], lines 16-17; Paragraph [0024], lines 6-10; Paragraph [0032], lines 3-5; The Examiner gives a broad interpretation of collecting a response packet which stores in a storage medium):

blocking an attack packet transmitted to the system and a first response packet output from the system as a response to the attack packet, if a system invasion sensing signal is received;

generating a second response packet into which a watermark is inserted, in response to the attack packet, and transmitting the second response packet to a system corresponding to the source address of the attack packet; and

receiving a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, tracing back the transmission path of the second response packet and identifying the location of the attacker system.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang et al., "Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework", obtained from *http://seclab.cs.ucdavis.edu/papers/2001-03-watermark-ifipsec.pdf* , March 2001, Pages 1-16, herein after SWT in view of Comay (U.S. Patent 6,363,489).

Claim 1

SWT discloses a traceback connection apparatus comprising:

a response packet generation unit, which generates a second response packet into which a watermark is inserted, in response to the attack packet, and transmits the second response packet to a system corresponding to the source address of the attack packet (Pages 9-10, section 4); and

a path traceback unit, which receives a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, traces back the transmission path of the second response packet and identifies the location of the attacker system (Pages 9-10, section 4);

SWT does not disclose a packet blocking unit.

Comay discloses a packet blocking unit, which if a system attack sensing signal is received, blocks an attack packet transmitted to a system and a first response packet output from the system in response to the attack packet (Column 3, lines 52-59; Column 6, lines 39-67). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify an apparatus

of SWT by including the packet blocking unit of Comay because it would prevent damage to a system from an unauthorized user entering a network.

Claim 2

SWT and Comay disclose the apparatus in claim 1 as described above.

Comay further discloses the apparatus of claim 1, further comprising:

an attack detection unit, which if a system attack by an external attacker is sensed, outputs an attack sensing signal containing the IP addresses of the source and destination of the attack path and the port number (Column 5, lines 15-30).

Claim 3

SWT and Comay disclose the apparatus in claim 1 as described above.

Comay further discloses the apparatus of claim 2, wherein the attack detection unit senses a system attack by the external attacker by investigating log files of the system, log files of a network, and whether or not a predetermined system file has been changed, and based on the log file of the system, identifies the IP address of the source and port number of the attack packet (Column 5, lines 15-30).

Claim 4

SWT and Comay disclose the apparatus in claim 1 as described above.

Comay discloses the apparatus of claim 2, wherein the packet blocking unit comprises:

a signal reception unit, which receives the attack sensing signal (Column 5, lines 15-30);

a packet identifying unit, which identifies the attack packet and the first response packet based on the IP addresses and the port number (Column 5, lines 15-30); and

a blocking unit, which blocks the attack packet and the first response packet (Column 3, lines 52-59; Column 6, lines 39-67).

Claim 5

SWT and Comay disclose the apparatus in claim 1 as described above.

SWT further discloses the apparatus of claim 1, further comprising:

a watermark detection unit, which if a packet containing a watermark from an external network is received, transmits a detection packet containing the path information of the received packet to a system of the external network which inserted the watermark (Pages 7-8, section 3.1).

Claim 6

SWT and Comay disclose the apparatus in claim 1 as described above.

SWT further discloses the apparatus of claim 5, wherein the watermark detection unit comprises:

a detection unit, which detects a watermark contained in a packet received from the outside (Pages 12-14, section 4.3);

a detection packet generation unit, which if a watermark is detected, generates a detection packet containing the IP addresses of the source and destination and port number of the received packet (Pages 12-14, section 4.3); and

a packet transmission unit, which transmits the generated detection packet to a system that first inserted the watermark to the packet (Pages 12-14, section 4.3).

Claim 7

SWT and Comay disclose the apparatus in claim 1 as described above.

SWT further discloses the apparatus of claim 1, wherein the path traceback unit traces back the location of an attacker system based on the IP addresses of the source and destination and port number contained in the one or more received detection packets (Pages 9-10, section 4).

Claim 8

SWT discloses a traceback connection method comprising:

generating a second response packet into which a watermark is inserted, in response to the attack packet, and transmitting the second response packet to a system corresponding to the source address of the attack packet (Pages 9-10, section 4); and

receiving a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, tracing back the transmission path of the second response packet and identifying the location of the attacker system (Pages 9-10, section 4).

SWT does not disclose a method of blocking an attack packet transmitted to the system and a first response packet output from a system in response to the attack packet, if a system invasion sensing signal is received.

Comay discloses the method of blocking an attack packet transmitted to the system and a first response packet output from a system in response to the attack packet, if a system invasion sensing signal is received (Column 3, lines 52-59; Column 6, lines 39-67). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the method of SWT by including the method of Comay because it would prevent damage to a system from an unauthorized user entering a network.

Claim 9

SWT and Comay disclose the steps in claim 8 as described above.

Comay further discloses the method of claim 8, further comprising:

outputting an attack sensing signal containing the IP addresses of the source and destination of the attack path and the port number before the blocking, if a system attack by an external attacker is sensed (Column 5, lines 15-30).

Claim 10

SWT and Comay disclose the steps in claim 8 as described above.

Comay further discloses the method of claim 9, wherein the blocking comprises:

receiving the attack sensing signal (Column 5, lines 15-30);

identifying the attack packet and the first response packet based on the IP addresses and the port number (Column 5, lines 15-30); and

blocking the attack packet and the first response packet (Column 3, lines 52-59; Column 6, lines 39-67).

Claim 11

SWT and Comay disclose the steps in claim 8 as described above.

SWT further discloses the method of claim 8, further comprising:

transmitting a predetermined detection packet to a system of the external network which inserted the watermark, if a packet containing a watermark from an external network is received (Pages 7-8, section 3.1).

Claim 12

SWT and Comay disclose the steps in claim 8 as described above.

SWT further discloses the method of claim 11, wherein transmitting a detection packet comprises:

detecting a watermark contained in a receive packet (Pages 12-14, section 4.3);

If the watermark is detected, generating a detection packet containing the IP addresses of the source and destination and port number of the received packet (Pages 12-14, section 4.3); and

transmitting the generated detection packet to a system that first inserted the watermark to the packet (Pages 12-14, section 4.3).

Claim 13

SWT and Comay disclose the steps in claim 8 as described above.

SWT further discloses the method of claim 8, wherein the tracking back the transmission path comprises:

tracking back the location of an attacker system based on the IP addresses of the source and destination and port number contained in the one or more received detection packets (Pages 9-10, section 4).

Claim 14

SWT and Comay disclose the steps in claim 8 as described above.

SWT further discloses a computer readable medium having embodied thereon a computer program for executing a traceback connection method comprising (Figure 1, Router):

blocking an attack packet transmitted to the system and a first response packet output from the system as a response to the attack packet, if a system invasion sensing signal is received;

generating a second response packet into which a watermark is inserted, in response to the attack packet, and transmitting the second response packet to a system corresponding to the source address of the attack packet; and

receiving a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, tracing back the transmission path of the second response packet and identifying the location of the attacker system.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory

obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-13 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-3 of copending Application (Publication No: US20040049695 A1). Although the conflicting claims are not identical, they are not patentably distinct from each other because for the following reasons.

Claims 1-7 map into claim 1 of the copending application.

Claim 8 maps into claim 2 of the copending application.

Claims 9-13 map into claims 2 and 3 of the copending application.

Conclusion

The Tanaka (Publication No.: 20010026616 A1) discloses an electronic watermark data insertion apparatus and electronic watermark data detection apparatus.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le
December 11, 2006

WALTER D. GRIFFIN
SUPERVISORY PATENT EXAMINER